

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF TEXAS  
TYLER DIVISION

UNITED STATES OF AMERICA	§	
Plaintiff,	§	
	§	
v.	§	NO: 6:23-CV-00618
	§	
\$2,305,233.88 IN UNITED STATES	§	
CURRENCY	§	
Defendant.	§	

**AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE**

I, Brad Schley, after being duly sworn, depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Senior Special Agent (SSA) with the United States Secret Service (USSS) and have been so employed since September 2001. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, specifically those related to the passing of counterfeit United States currency, money laundering, and wire fraud. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have conducted investigations resulting in the arrest of suspects and seizures of criminally derived property. I am an investigative and law

enforcement officer of the United States, in that I am empowered by law to conduct investigations and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

2. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses.

### **PROPERTY FOR FORFEITURE**

3. This Affidavit is made in support of a civil forfeiture complaint concerning \$2,305,233.88 in Citibank account 50050912 (TARGET ACCOUNT), Check No. 191331931 seized on or about October 12, 2023 in Sioux Falls, South Dakota, pursuant to a seizure warrant.

### **LEGAL AUTHORITY FOR FORFEITURE**

4. The funds to be forfeited represent proceeds of a fraudulent cryptocurrency investment scheme that often utilizes spoofed domains. The term “spoofed” refers to domain spoofing and involves a cyberattack in which fraudsters and/or hackers seek to persuade consumers that a web address or email belongs to a legitimate and generally trusted company, when in fact it links the user to a false site controlled by a cybercriminal. In particular, the unknown scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to United States-based victims, including victims located in Tyler, Texas, which is located within

the Eastern District of Texas. Scammers then fooled victims into “investing” in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal the victims’ money.

5. This type of scam is often identified as “pig butchering” (derived from the Chinese phrase used to describe this scheme) and involves scammers spending significant time getting to know, targeting, and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds through a provided BTC, USDT, ETH or USDC deposit address, and are further told they can expect to make a sizeable return on their investments. As initial smaller investments are made, the spoofed websites falsely display a significant increase in the victim’s account balance, which entices the victim to continue making investments, which typically ends with a final large deposit or transaction. When the victim attempts to make a withdrawal, the scammers attempt to coerce the victims to make additional investments. These tactics can include requesting additional investments due to “significant profits” gained on the account or other reasons such as freezing the account due to “taxes owed” or “suspicious behavior.” Regardless of how the scammers attempt to solicit additional investments from the victims, the victims are unable to retrieve any portion of their investment.

6. I believe the above-listed property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because the property was involved in or traceable to property involved in money laundering in violation of 18 U.S.C §§ 1956 or 1957, or constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)).

7. Any property, real or personal, which was involved in a transaction in violation of 18 U.S.C. §§ 1956 or 1957 or any property traceable to such property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

8. 18 U.S.C. § 1956 (a)(1) makes it a crime to knowingly conduct or attempt to conduct a “financial transaction” with proceeds from “specified unlawful activity” (SUA) with specific intent to: promote the SUA, conceal, or disguise the source, origin, nature, ownership, or control of the proceeds; or evade reporting requirements.

9. The purpose of “money laundering” as defined by 18 U.S.C. § 1956 is to disguise illicit nature of funds by introducing it into legitimate commerce and finance thereby making them “clean.” This financial process is most commonly conducted using three steps referred to as “placement,” “layering,” and “integration.” Typically, the “placement” phase of this financial process takes place when proceeds from illicit sources are placed in a financial institution or business entity. “Layering” takes place when these funds are then used in seemingly legitimate commerce transactions which makes the tracing of these monies more difficult and removed from the criminal activity from which they are a source. Finally, the “integration” phase is when these funds are then used to

promote the unlawful activity or for the personal benefit of the money launderers and others.

10. I also believe that this property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because the property constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 (wire fraud) or a conspiracy to commit such offense (18 U.S.C. § 1349). Wire fraud is an SUA. 18 U.S.C. § 981(a)(1)(C).

11. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 or a conspiracy to commit such (18 U.S.C. § 1349) is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

12. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

- a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;
- b. It is not a defense that those funds have been removed and replaced by other funds; and
- c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

13. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the “guilty” property had been kept.

### **FACTS SUPPORTING FORFEITURE**

14. The United States is investigating a pig butchering scheme involving a fraudulent cryptocurrency investment scheme that utilizes spoofed domains. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud), and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments).

15. The case involves the laundering of proceeds obtained from victims of the fraudulent scheme. Part of the money laundering scheme was to funnel proceeds from pig butchering victims through the various business accounts to accounts located abroad. One business, identified as Elights Trading Inc., held a bank account that served as a funnel account and received fraud proceeds from bank accounts held in the names of the pig butchering victims.

16. The TARGET ACCOUNT is a business checking account. Bank records show FEI LIAO as the owner of ELIGHTS TRADING INC with a business address of 16269 Sierra Ridge Way, Hacienda Heights, California 91745. As of November 8, 2023, Elights Trading Inc has no identifiable Internet presence. A review of bank and business records also failed to identify any website relating to the business of ELIGHTS TRADING INC.

17. Local law enforcement officers who are familiar with the immediate area of 16269 Sierra Ridge Way, Hacienda Heights, California reported to USSS investigators that it is a residential area and with no readily identifiable businesses located at the address.

18. The opening documents for the TARGET ACCOUNT indicate Fei Liao opened the business bank account identifying Elights Trading Inc. as a corporation with an annual gross revenue of \$500,000 and an annual net profit of \$100,000. The records indicate the business (Elights Trading) is an import/export company that will purchase items in bulk in a wholesale price and resell to retailers at a smaller quantity at retail price. The bank records indicate that Liao selected “No” to the following account opening questions from Citibank:

- a. Will you provide check cashing services, foreign currency services, money transmission services or sell financial instruments totaling more than \$1,000?
- b. Will you deposit or withdraw more than \$40,000 in cash, money orders or travelers checks each month?
- c. Will you hold or transact any funds in this account that belong to one or more of your customers and are not part of your business’ operating funds? (e.g., Will any funds be held as an investment for a client, or used to settle funds similar to an investment service or trust agreement?)

19. The transactions for the TARGET ACCOUNT indicate the account received deposits from individuals beginning on or about September 7, 2023, through September 15, 2023, totaling approximately \$2,837,132.88. The table below represents the identified remitters, date, and amount of each transaction:

DATE	REMITTER/VICTIM	AMOUNT
9/7/23	T.G.	\$230,000.00
9/7/23	J.Z.	\$120,000.00
9/7/23	J.S.	\$100,000.00
9/7/23	G.C.	\$93,673.88
9/8/23	A.P.	\$660,000.00
9/8/23	Y.I.	\$355,000.00
9/8/23	P.M.	\$97,000.00
9/8/23	C.A.	\$95,000.00
9/8/23	V.V.	\$68,000.00
9/8/23	A.M.	\$40,000.00
9/11/23	S.M.	\$130,000.00
9/11/23	D.H.	\$100,000.00
9/11/23	A.P.	\$50,000.00
9/11/23	D.K.	\$170,000.00
9/12/23	D.B.	\$110,030.00
9/12/23	D.W.H.	\$53,000.00
9/12/23	K.S.	\$50,000.00
9/13/23	M.A.D.	\$25,000.00
9/13/23	A.A.	\$290,390.00

20. USSS investigators identified a significant portion of the remitters of the wires funding the TARGET ACCOUNT noted above and conducted interviews. The persons interviewed were identified as victims of a fraudulent investment scheme, mainly investments into what victims thought was cryptocurrency. Essentially, most victims reported to have met someone online or through a “wrong number call or text message.” The victims continued to communicate with the unknown persons and the conversation turned to investments into cryptocurrency or other items such as gold. The victims



reported to receive a link or directions to download a spoofed application that mimicked a legitimate cryptocurrency exchange. The victims were able to create an “account” at these spoofed domains or aps and the operators of these spoofed domains were able to manipulate the account balances to reflect the “deposits” made by victims. Most of the time, victims tested the system to ensure it worked by withdrawing a small portion of their smaller initial investment. Once they were able to see that they were able to withdraw the funds, they were enticed to invest again and often did so with a large sum of funds. The victims reported that when they attempted to conduct a larger withdrawal, they were notified that they needed to pay taxes on their earnings or other nonsensical fees. Some victims did go through the process of paying taxes and other nonsensical fees, only to have their accounts locked or were continued to be informed of the need to pay additional fees. Ultimately, these victims were not able to have access to their funds and sustained significant losses.

21. For example, Investigators interviewed victim K.S. regarding his transaction of \$50,000.00 to the TARGET ACCOUNT. K.S. stated that on or about August 7, 2023, he received a “wrong number” telephone call from a person who identified herself as Sofia Buterin using telephone number 626-525-3735. K.S. stated that Buterin befriended K.S. and they communicated daily beginning on or about August 7, 2023. K.S. stated that Buterin even provided him with a photo of a Massachusetts driver’s license, bearing number S36102955, a white female, and the name Sofia Dmitrievich Buterin with date of birth July 15, 1991. K.S. stated the conversation then

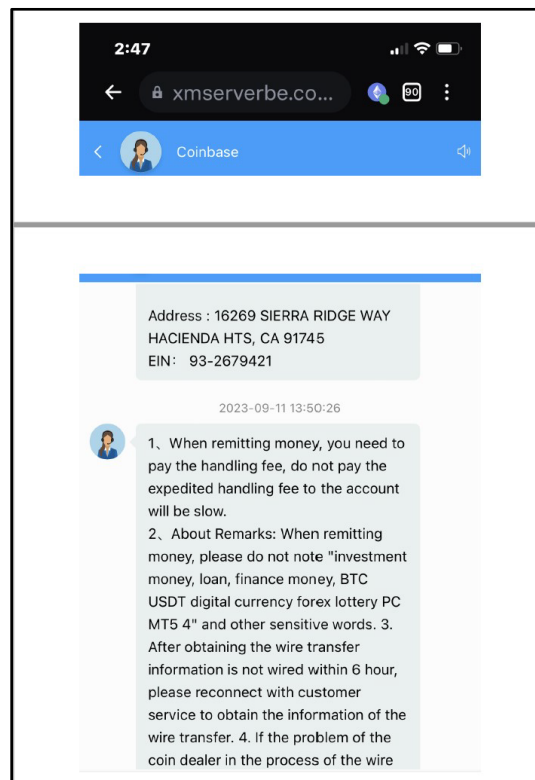
turned into how Buterin could assist K.S. in making money by investing in cryptocurrency. K.S. stated that he complied by initially investing \$5,000 using the UPHOLD exchange, where he earned a profit in a very short time-period. Having gained his trust, K.S. then was willing to invest \$50,000 and Buterin provided him with the banking information for Elights Trading Inc. at Citibank. K.S. stated after he sent the funds to Elights Trading Inc., he was instructed to wait two to three days until a seller was located to send him USDT. K.S. stated he waited two to three days and never received his USDT.

22. Investigators queried official driver's license records for the state of Massachusetts and discovered that the driver's license bearing Buterin's identity is fictitious, as the driver's license is registered to a male individual born in the year 1966.

**Victim D.B.**

23. Investigators interviewed victim D.B. regarding his transaction of \$110,030.00 to the TARGET ACCOUNT. D.B. confirmed his transaction to Elights Trading Inc. and stated he invested in cryptocurrency using his Coinbase account and a Coinbase Application he downloaded on his phone. D.B. stated he funded his Coinbase account from his Bank of America account, and was just an investor, buying BTC low and selling BTC high. D.B. stated that Coinbase's fees were expensive and consuming most of his earnings, and that Coinbase Pro, which has lower fees, is too difficult to navigate. D.B. stated that while he was using his Coinbase Application, he utilized the support button to inquire about trading with a private coin supplier to avoid expensive

transaction fees and improve his return on investment. D.B. claimed that he received the instructions and bank account information for Elights Trading Inc. from the support staff on the Coinbase Application. The following image is a screenshot D.B. provided to investigators indicating he received the bank information for the Target Account from the spoofed Coinbase Application:



24. Investigators obtained permission to view D.B.'s phone that is used to access the Coinbase application. The web address displayed as coinbass-vip.com, which was utilized to trick users into thinking they were utilizing the legitimate coinbase.com platform. The ending of "vip" is the same method utilized in the aforementioned domain

name provided by EDTX victims H.J. and K.J. when they accessed domains www.achainjp.vip and www.aczkoin.vip.

25. USSS investigators obtained confirmation from known Coinbase employees who confirmed the application used by victim D.B. was not a legitimate Coinbase application and/or domain.

**Victim A.M.**

26. Investigators interviewed victim A.M. regarding the \$40,000 transaction remitted to the TARGET ACCOUNT. A.M. stated he belongs to a crypto investment group on the communication platform Telegram. A.M. stated he was provided the bank account information for the TARGET ACCOUNT in the Telegram investment group.

**Victim T.G.**

27. Investigators interviewed victim T.G. regarding the \$230,000 transaction remitted to the TARGET ACCOUNT. T.G. stated he met a friend on Facebook in or about May 2023, but has never met this individual face to face. T.G. stated his new female friend portrayed herself as being very wealthy and T.G. inquired how he could invest money to earn a large and safe return. T.G. stated that his friend provided a link to Telegram where he was led to believe he was working with employees of OKEX, a cryptocurrency exchange. T.G. stated he received instructions via Telegram regarding investments, including the information for the Target Account. T.G. stated he believed he was purchasing options in cryptocurrency and not specific cryptocurrency coins such as Bitcoin. T.G. stated he has invested approximately \$850,000 in total by sending to

other bank accounts he received from the OKEX Telegram communications. T.G. stated he has only requested small withdrawals from his investment and has received only a few thousand dollars and has not made any large withdrawal requests.

28. One of the additional bank accounts received by T.G. included a JP Morgan Chase bank account number ending in 2181. Investigators contacted JP Morgan Chase bank investigators who advised that this account was under investigation by JP Morgan Chase.

**Victim C.A.**

29. Investigators interviewed victim C.A. who confirmed her transaction of \$95,000.00 to the TARGET ACCOUNT she sent on September 8, 2023. C.A. stated she was contacted by a family friend via Facebook messenger. C.A. stated she does not know this family friend and has not met them in person. C.A. stated the conversation with the family friend included investments and how to obtain a significant return over a short period. C.A. told investigators that the family friend referred her to Elights Trading Inc. at telephone number 518-898-1054 to invest in cryptocurrency. C.A. stated once she was referred to Elights Trading Inc., she believed she was communicating with a customer service representative and/or employee of Elights Trading Inc. C.A. stated she has no experience investing in cryptocurrency, so she trusted the information she was receiving from Elights Trading Inc. C.A. informed investigators that in her discussions with Elights Trading Inc., she was expected to receive 15-20% on her investment within a few days of her deposit to the Target Account. C.A. stated she was not provided with any

account number, log-in credentials, or other account information regarding her investment. C.A. stated that prior to speaking with investigators on September 26, 2023, she was notified by Elights Trading Inc. that her funds would be returned to her because there was an issue with the TARGET ACCOUNT. C.A. stated Elights Trading Inc. instructed her to provide C.A.'s bank with wire recall instructions. At the time of the interview with investigators, C.A. stated her funds had not been returned to her bank account.

30. Complaints have also been filed with the FBI's Internet Crime Complaint Center, [www.IC3.gov](http://www.IC3.gov), by victims who have suffered financial losses by this scam by sending funds to the TARGET ACCOUNT. A review of an IC3 report dated September 18, 2023, was made by H.J., and reported that he attempted to send \$500,000.00 from his account to the TARGET ACCOUNT so that he could repay a temporary loan for trading cryptocurrency. H.J. reported that he invested \$116,000.00 in what he was made to believe was a crypto exchange at [www.trxxw.com](http://www.trxxw.com) and was informed by unknown members of the criminal syndicate that he could not recover his investment until he pays his loan in full. This activity is very similar to the activity reported by EDTX victims K.J. and H.J.

### **Target Account Withdrawal Activity**

31. Investigators obtained bank records regarding the TARGET ACCOUNT and discovered that the withdrawal activity included bank fees and one outgoing wire transaction in the amount of \$530,199.00 on September 8, 2023, that was sent to recipient

Paretone Capital Cayman Ltd, account number ending in 1564. Paretone Capital Cayman Ltd advertises the company is an investment platform focusing on digital assets that operates in Hong Kong, Singapore, and the United States. This investigation has identified additional shell companies receiving proceeds of this fraud scheme. These shell companies have accounts at numerous financial institutions and some of them also have sent funds to Paretone Capital Cayman Ltd.

32. Other withdrawal activity was minimal and involved transactions less than \$2,000.00 total.

33. On September 14, 2023, investigators provided a freeze letter request to Citibank for assets and monies in the TARGET ACCOUNT to be frozen. Citibank employees informed investigators that the TARGET ACCOUNT's balance is approximately \$2,305,233.88.

34. On or about October 12, 2023, USSS investigators obtained and served a federal seizure warrant for any and all funds held in the Target Account.

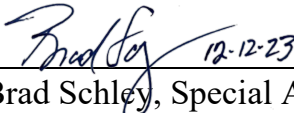
35. On or about October 24, 2023, USSS investigators received a Citibank cashier's check bearing number 191331931 that was drawn on the TARGET ACCOUNT in the amount of \$2,305,233.88.

### **CONCLUSION**

36. I submit that this affidavit supports the forfeiture of all funds, monies, and other things of value up to \$2,305,233.88 seized from Citibank Bank account 50050912 in the name of ELIGHTS TRADING INC.

37. The seized property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A) because it is any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. §§ 1956 and 1957, or any property traceable to such property, and pursuant to 18 U.S.C. § 981(a)(1)(C) because it is any property, real or personal, which constitutes or is derived from proceeds traceable to a violation of any offense constituting a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7)), namely, a violation of 18 U.S.C. § 1343, or a conspiracy to commit such offense (18 U.S.C. § 1349).

As provided in 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

 12-12-23  
\_\_\_\_\_  
Brad Schley, Special Agent  
U.S. Secret Service